NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Severed data line repaired after cut stymies communication in Jamestown area. A severed data line east of Jamestown, North Dakota, caused communication problems for the Jamestown area June 14. A Century Link fiber line was cut late in the morning. about 10 miles west of Valley City causing landline telephone problems in the region, according to a marketing manager with Dakota Central Telecommunications. A spokeswoman for Century Link said the cable was completely repaired within 7 hours. She said the cable was cut by a construction crew, and that customers in Jamestown and Valley City were affected. The severed line made it so many Jamestown-area residents could not make calls from landline phones, while calls between cellphones were still able to connect. This meant local residents could not call 9-1-1 from a landline. The assistant Stutsman County emergency manager and 9-1-1 coordinator said 9-1-1 calls from cellphones were immediately rerouted to State Radio in Bismarck and landline 9-1-1 calls were answered in Jamestown by using other seven-digit emergency lines that were dispersed to the public. Source: http://www.jamestownsun.com/event/article/id/163023/

$700K contract awarded for repair of Velva levees. The U.S. Army Corps of Engineers awarded a contract for the repair of levees in Velva, North Dakota, that were damaged during historic Souris River flooding during summer 2011. A Maple Grove, Minnesota, company landed the $700,000 project. Construction is to begin in July and wrap up this fall. Source: http://www.cbsnews.com/8301-505245_162-57449701/$700k-contract-awarded-for-repair-of-velva-levees/

Regional

(Minnesota) **Three guilty in massive Ponzi scheme.** Jurors in Minneapolis June 12 found three men guilty of helping a convicted fraudster pilfer the savings of more than 700 investors in a Ponzi scheme. All three were found guilty of all the charges resulting from the $194 million scheme — the second-largest Ponzi scheme in Minnesota history. A man who claimed to be among the top portfolio managers in the nation was convicted of a variety of fraud, money-laundering, and tax charges. An entrepreneur and former coin dealer was convicted of fraud and money-laundering charges; attempting to mislead the government about two foreign currency transactions; and several tax charges. A Minneapolis huckster — whose "Follow the Money" radio talk-show program lured the most investors — was found guilty of fraud and money laundering counts. The scheme evolved from currency swaps the leader of the scheme was running through several commodities and futures brokers. He claimed in 2006 to have found the Holy Grail with two Swiss firms: Crown Forex SA and JDFX Technologies. By partnering with these firms and others, the schemer and his associates claimed they could produce steady, double-digit returns with no risk to principal. Two of the defendants pitched the investment strategy on a Christian shortwave network and broadcast radio. One of them bought time on more than 200 stations nationwide and brought in about two-thirds of the investors. The third defendant solicited investors among the wealthy clientele of his investment advisory company, Oxford Private Client Group, and made presentations at investment seminars. He and associates in Minneapolis and Arizona raised about $47 million from 143

investors. In fact, the currency program was a fraud from top to bottom and the three defendants knew it but never informed their investors, prosecutors argued. The scam became public in July 2009. Source: http://www.startribune.com/local/158578925.html?page=all&prepage=1&c=y#continue

National

Disaster awaits U.S. power grid as cybersecurity lags. Security technology used by U.S. electric utilities is flawed and could increase the odds of computer intrusions or sabotage, warns the co-chair of the North American Energy Standards Board's (NAESB) Critical Infrastructure Committee. NAESB scheduled a committee vote June 14 to decide when the digital certificates it authorizes should expire. Since even carefully designed algorithms have flaws that will be discovered over time, which happened with the MD5 algorithm in 1995 and the SHA-1 algorithm in 2005, a shorter period is considered more secure. Two companies, Open Access Technology International and GlobalSign, which are authorized by the NAESB to issue digital certificates to the industry, argue that a 30-year expiration for digital certificates is sufficient. The co-chair of the NAESB Critical Infrastructure Committee said, "I'd be advocating for something smaller like 10 or 5 (years) but that's not on the table at the moment." The president of NAESB said it is unclear whether the revised digital certificate standard will apply to Web interfaces or embedded supervisory control and data acquisition systems — which directly control power and gas transmission — as well. Source: http://news.cnet.com/8301-1009_3-57452863-83/disaster-awaits-u.s-power-grid-as-cybersecurity-lags/

Utilities need to invest more in smart grid cybersecurity, regulators warn. State regulators warned utilities they must increase investment in cybersecurity protections for the smart grid. In a paper issued the week of June 11, the National Association of Regulatory Utility Commissioners (NARUC) said the move to a smart grid will increase cybersecurity vulnerabilities. "We find ourselves at a critical juncture … Cybersecurity must encompass not only utility-owned systems, but some aspects of customer and third party components that interact with the grid, such as advanced meters and devices behind the meter," the paper stressed. The paper proposed a series of questions State commissions should ask utilities regarding cybersecurity. The questions seek answers to see if utilities are planning cybersecurity investments with sound procurement strategies, and implementing policies and personnel to deal with potential challenges. Source: http://www.infosecurity-magazine.com/view/26275/

International

Plains shuts Alberta oil pipeline after leak. Plains Midstream Canada said June 8 it shut part of a pipeline in west-central Alberta, Canada, after crude leaked into a large river system just as the company was close to finishing its cleanup of a big year-old spill in the province. Plains Midstream, a unit of Houston-based Plains All American, estimated that 1,000-3,000 barrels of light, sour crude — oil that has a high sulfur content — leaked from a 12-inch line on its Rangeland south system into a tributary of the Red Deer River, a large waterway that runs

across south-central Alberta. Stream flows were high due to heavy rainfall and snow melt from the Rocky Mountains, which will make cleanup tricky. The company said it has deployed booms at a reservoir that doubles as a resort area and has brought in drinking water for local residents as a precaution. Source: http://in.reuters.com/article/2012/06/08/plains-pipeline-alberta-idINL1E8H82AY20120608

Banking and Finance Industry

Banks: Hackers more aggressive in attacking customer accounts. A survey of large financial institutions shows they faced more attacks by hackers to take over customer banking accounts in 2011 than in the 2009 and 2010, and about one-third of these attacks succeeded, Network World reported June 14. The total number of attacks to try and break in and transfer money out of hacked accounts was up to 314 during 2011, according to the Financial Services Information Sharing and Analysis Center (FS-ISAC), which released findings of its survey of 95 financial institutions and 5 service providers. That number marks an increase from 87 attacks against bank accounts in 2009 and 239 in 2010. The survey was conducted by the American Bankers Association. The actual dollar losses taken by the financial institutions last year was $777,064, down from a high of $3.12 million in 2010. Dollar loss for customers was $489,672 in 2011, as compared with $1.16 million in 2010. Source: http://www.computerworld.com/s/article/9228139/Banks_Hackers_more_aggressive_in_attacking_customer_accounts

TSP executive director gives update on data breach. It has been nearly 3 weeks since the Thrift Savings Plan (TSP) board announced a data breach of 123,000 TSP accounts, and since then, the board has been fielding questions from participants, Congress, and the media. One of the most common questions: Is my account safe? If a participant did not receive a letter from the TSP board, their account is not affected by the breach, said the executive director of the TSP. In July 2011, a breach at a TSP contractor — Serco, Inc. — compromised the data of 123,000 accounts. Most of the data accessed included Social Security numbers only. However, of those 123,000, about 43,000 participants had their names, addresses, Social Security numbers and other information — possibly bank routing numbers — also compromised. Source: http://www.federalnewsradio.com/180/2901150/TSP-executive-director-gives-update-on-data-breach

Payment processor finds more trouble from breach. A major payment processor suspects the fallout from a recent security breach may be worse than it initially believed. Global Payments Inc. raised the red flag June 12, more than 2 months after it first reported computer hackers may have stolen data from as many as 1.5 million credit and debit card accounts in North America. At that point, the company had concluded the crooks had not taken anyone's name, address, or Social Security numbers. However, after its investigators dug deeper into the intrusion, Global Payments discovered the bandits also may have pried into computers storing the personal information of various merchants applying to have their sales processed. Besides names, addresses, and Social Security numbers, Global Payments also stores drivers' license numbers and banking account numbers of merchants, according to regulatory filings. The

company said it still does not believe any personal information was taken from the up to 1.5 million card accounts cited in its original report of the theft. The data taken from the cards is believed to be mostly account numbers, expiration dates, and security codes. Other key details remain murky because Global Payments still has not identified the merchants and banks entangled in the mess, nor estimated how many people may now be vulnerable to identify theft. Global Payments said it believes "this incident is contained." The company expects to have a better handle on how much the hacking will cost by July 26. So far, Global Payments said there have been no fraudulent charges tied to the breach. Source: http://www.businessweek.com/ap/2012-06/D9VBVDFO0.htm

(New Mexico; Oklahoma; Texas) **Mexico cartel accused of laundering money at U.S. racetracks.** The unlikely marriage of a violent Mexican drug cartel and U.S. quarter horses has apparently ended with the arrest of one of the top suspected members of the Zetas gang. The cartel member, his wife, and five associates were charged June 12 in Austin, Texas, with using horses to launder millions of dollars in drug proceeds. They were taken into U.S. custody after scores of FBI agents raided stables and ranches near Ruidoso, New Mexico, and Lexington, Oklahoma. Working on a tip from more than 2 years ago, law enforcement officials learned the Zetas were allegedly laundering up to $1 million a month in the high circles of American-bred quarter horses. An additional 11 suspects were being sought. The two-State takedown marked the first known time a cartel has allegedly used such a tactic. The indictment alleges when drug-smuggling profits returned to the Zetas in Mexico in "bulk cash shipments," they were delivered to "plaza bosses for counting and distribution." To launder the profits, the cartel turned to "investments in racing quarter horses purchased via bulk currency payments, wire transfers, structured deposits, and bulk currency deposits." The cartel member and his wife allegedly handled things on the U.S. side, creating several corporations — Tremor Enterprises, 66 Land, and Zule Farms — to facilitate moving the money. Those arrested June 12 and those who remain at large, face up to 20 years in prison, as well as fines and other damages of $20 million and more. Source: http://www.latimes.com/news/nationworld/nation/la-na-cartel-horses-20120613,0,2069688.story

Chemical and Hazardous Materials Sector

(Pennsylvania) **EPA reassesses site contaminant.** Environmental Protection Agency (EPA) officials proposed installing special ventilation systems in 11 more homes near the Crossley Farm Superfund Site in Hereford Township, Pennsylvania, the Reading Eagle reported June 14. After a reassessment of the toxicity of a carcinogen contaminating the area's groundwater in fall 2011, the EPA concluded the contaminant, trichloroethylene (TCE), is 10 times more toxic than officials originally believed. The standard for safe air levels was lowered to 2 micrograms per cubic meter from 20. With the new standard, 13 homes in the township required remediation of TCE, according to EPA officials. Experts said the airborne TCE is evaporating out of groundwater where TCE levels are 140,000 times the acceptable limit for drinking water. EPA measures the vapor levels from soils beneath homes likely to be affected. Mitigation systems will be installed at no cost, but residents will have to pay related electric costs of $5 to $15 per month. According to the EPA Web site, TCE levels as high as 700,000 micrograms per liter have

been measured in the groundwater. The remedial project manager for the EPA has said it could take 30 years to clean the groundwater, which is being pumped to the surface and decontaminated. Source: http://readingeagle.com/article.aspx?id=392781

Nuclear panel must weigh risks of long-term storage, court rules. A federal appeals court ruled June 8 the Nuclear Regulatory Commission (NRC) must consider the environmental and safety issues involved with long-term storage of radioactive wastes at nuclear power plants when it renews operating licenses. The ruling by the U.S. Court of Appeals in Washington, D.C., underscores the growing problem the nuclear energy industry faces as it continues to generate new waste and has no place to send it. The three-judge panel ruled the NRC evaluations have been deficient because the commission has failed to consider future risks when it has determined spent fuel can be stored for 60 years at plant sites. It also said the NRC has been wrong in not weighing the possibility that the radioactive fuel may have to stay where it is permanently, because the federal government may never have a nuclear dump for the spent fuel. Source: http://www.latimes.com/news/nation/nationnow/la-na-nn-nuclear-ruling-20120608,0,1477559.story

Official says EPA prepared in 'near future' to use TSCA authority to restrict chemicals. The U.S. Environmental Protection Agency (EPA) is prepared to see "in the near future" whether it can use authority the Toxic Substances Control Act (TSCA) provides to ban or restrict chemicals, the agency's senior chemicals and pesticide official said June 7. "We will try and exercise some muscle we have not exercised for decades," EPA's acting assistant administrator for chemical safety and pollution prevention told State officials attending an Environmental Council of the States' conference. Section 6 of the TSCA provides the EPA with the authority to ban or restrict chemicals. The agency has not sought to use its Section 6 authority since 1991, when an appellate court overturned the agency's attempt to ban asbestos. "We will find out if it is as hard to use as is said," the EPA administrator said. Source: http://www.bna.com/official-says-epa-n12884909957/

Commercial Facilities

(Texas) **Chemical spill shuts down Industrial Blvd. in Colleyville.** Industrial Boulevard in Colleyville, Texas, was shut down June 13 when 275 gallons of sulfuric acid spilled from a self-storage facility. A hazardous materials team used clay to absorb the acid and contain the spill that occurred inside Metroplex Self Storage. Some of the chemical spilled onto the roadway and a small amount leaked into a storm drain, officials said. They said a damaged valve was to blame for the sulfuric acid spill, which had 93 percent concentration. The acid is used to treat water. The road was still closed in the early evening. Officials said it would remain closed until clean-up was complete. One man was transported to a hospital for chemical burns on his hands and feet. Earlier news reports said two office buildings near the storage facility were evacuated, however, fire department officials said those businesses just closed early. Officials said the chemical posed no threat to nearby residents. Source: http://www.star-telegram.com/2012/06/13/4030122/chemical-spill-shuts-down-industrial.html

COMMUNICATIONS SECTOR

(Texas) **Copper thieves busted in Atascosa County.** Deputies in Atascosa County, Texas, caught three people trying to steal copper from a cell phone tower. The Atascosa County Sheriff's Office said the suspects were caught June 8 near Interstate 37 and Highway 281. According to investigators, the trio had roughly 1,500 feet of stolen copper wiring in their possession. Officials believed the trio was involved in several other copper thefts in the area. One of the suspects also had an active warrant for copper theft in Guadalupe County. Source: http://www.foxsanantonio.com/newsroom/top_stories/videos/vid_10610.shtml

CRITICAL MANUFACTURING

NHTSA recall notice - Honda Civic driveshaft separation. Honda announced June 13 the recall of 50,190 model year 2012 Honda Civic vehicles. During assembly, the process required to seat the driver's side driveshaft and set the retaining clip was not completed. As a result, the driveshaft may separate. If this occurs, the vehicle will have a loss of drive power and may roll away if the parking brake has not been set when the gear selector has been placed in the "park" position, increasing the risk of crash or pedestrian injury. Honda will notify owners, and dealers will inspect the driver's side driveshaft and install a new driveshaft, as needed. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V256000&summary=true&prod_id=1169768&PrintVersion=YES

Chrysler expands Jeep Liberty SUV recall. Chrysler expanded a recall regarding corrosion on Jeep Liberty vehicles to include the 2006 and 2007 model years after recalling the 2004 and 2005 model years in March, safety regulators and Chrysler said June 11. The two additional years add 137,176 U.S. vehicles to the recall. The recall affects vehicles in cold-weather areas that can sustain a rear suspension lower control arm fracture due to excessive conditions because of salt on roads in winter, according to a filing with the U.S. National Highway Transportation Safety Administration. Such a break could lead to loss of vehicle control and a crash. Source: http://www.reuters.com/article/2012/06/11/us-chrysler-recall-idUSBRE85A1AD20120611

DEFENSE/ INDUSTRY BASE SECTOR

Loss of oxygen incidents increase. New documentation says F-22 Raptor pilots experience a loss of oxygen at a rate at least 10 times higher than aboard any other U.S. Air Force (USAF) aircraft, WAVY 10 Portsmouth reported June 14. According to the report, the USAF reported 26.43 hypoxia or hypoxia-like incidents among F-22 pilots per 100,000 flight hours through May 31. The new information, released to Congress by a U.S. Senator from Virgina and a U.S. Representative from Illinois also states that following a 2011 USAF aircraft survey, a "majority of F-22 pilots surveyed did not feel confident" with breathing systems. Due to these results, the USAF ordered installation of charcoal filters in September 2011. According to the Air Force, a

study conducted by Boeing found the filter negatively impacted the F-22's breathing system for pilots. Source: http://www.wavy.com/dpp/military/loss-of-oxygen-incidents-increase

Attacks targeting U.S. defense contractors and universities tied to China. Researchers identified an ongoing series of cyberattacks targeting many high-profile organizations, including supervisory control and data acquisition (SCADA) security companies, universities, and defense contractors. The attacks are using customized malicious files to entice targeted users into opening them and starting the compromise. The campaign is using a series of hacked servers as command-and-control (C&C) points and researchers said the tactics and tools indicate the attackers may be located in China. The first evidence of the campaign was an attack on Digitalbond, a company that provides security services for industrial control systems. The attack begins with a spear-phishing e-mail sent to employees of the targeted company and contains a PDF attachment. In addition to the attack on Digitalbond, researchers found the campaign also hit users at Carnegie Mellon University, Purdue University, and the University of Rhode Island. Also, the Chertoff Group, a government consultant, and NJVC, a government contractor, were targeted. Alienvault identified similarities to the so-called Shady Rat attacks first publicized by McAfee in August 2011. The attackers are not hitting random targets with this campaign but are selecting their targets carefully. "According to the information collected, the targets of these campaigns are somehow related with the US government or US Defense contractors directly, providing different services such as authentication software/hardware, Industrial Control Systems security, or strategic consulting," a researcher at IOActive wrote in an analysis on the attacks. Source: http://threatpost.com/en_us/blogs/attacks-targeting-us-defense-contractors-and-universities-tied-china-061312

F-22's balky vests add clue in mystery of ailing pilots. A potentially faulty pressure vest is the latest clue in a year-long mystery over why U.S. Air Force pilots flying Lockheed Martin's F-22 Raptor keep getting dizzy and disoriented. Pilots were instructed to stop using the vest during routine flight operations as the Air Force works on a fix, the service's Air Combat Command said June 13. The vest, part of a "G suit" used to help pilots avoid blacking out during high-speed maneuvers, "increases the difficulty of pilot breathing under certain circumstances," according to a statement. Unable to explain episodes of dizziness, the Air Force is looking at everything from hoses, masks, and now G suits, to the coatings and adhesives used in the plane's radar-absorbing stealth skin. So far, all the engineers and investigators have not found a definitive cause. Source: http://www.bloomberg.com/news/2012-06-14/f-22-s-balky-vests-add-clue-in-mystery-of-ailing-pilots.html

Emergency Services

(New Jersey) **Coast Guard: Yacht blast hoax calls came from land.** The U.S. Coast Guard said two hoax calls reporting an explosion June 11 on a motor yacht off central New Jersey came from land and the rescue effort cost the agency at least $88,000 and lasted about 4 hours. An investigation began June 12 to determine who was responsible. The agency is offering a $3,000 reward. The caller reported the boat was 17 nautical miles east of Sandy Hook and had 21 people aboard including several people injured. The caller also claimed the vessel sank but

everyone aboard made it to life rafts. Authorities found no sign of any people or any distress in the water. The commander of Coast Guard Sector New York said more than 200 first responders assembled at the staging areas, and officials said several good Samaritans assisted authorities in the lengthy search. He noted hoax calls put the Coast Guard and other first responders at unnecessary risk and can interfere with the Coast Guard's ability to respond to actual distress at sea. Source: http://www.federalnewsradio.com/615/2900020/Coast-Guard-offers-reward-in-yacht-explosion-hoax-

Energy

(Texas) **Police: Man caught trying to steal copper from BTU.** A Breckenridge, Texas man was arrested June 10 after police said he was seen trying to steal copper wire from a Bryan Texas Utilities (BTU) facility. A BTU employee reported seeing a man enter a fenced storage lot and take copper wire, according to the police report. When a Bryan police officer arrived at the facility, the man was holding copper wire and tried to hide under a utility truck, the report stated. He was charged with theft of copper worth less than $20,000, a State jail felony punishable by up to 2 years in jail and a $10,000 fine, and criminal trespass, a Class A misdemeanor punishable by a up to a year in jail and a $4,000 fine. Although people have been caught stealing copper from BTU in the past, it has not been a major problem at the Atkins Street facility, said a spokesman for the city-owned utility company. Officials said they did not know the value of the copper the man allegedly tried to take. Source: http://www.theeagle.com/article/20120611/BC0102/120619915/1003/BC01

(Massachusetts) **2 men arrested after substation explosion.** Police arrested two men they initially thought might be injured or dead after they allegedly broke into an electrical substation in Haverhill, Massachusetts, to steal copper wire, causing a power outage. The two men were arrested June 8 on charges including breaking and entering, and attempted larceny. A May 30 explosion during the alleged break-in knocked out power to 2,700. Police thought the perpetrators might have been killed after coming into contact with 23,000 volts of electricity. They even searched with cadaver-sniffing dogs. Source: http://articles.boston.com/2012-06-09/news/32143450_1_electrical-substation-power-outage-explosion

Food and Agriculture

FDA urges removal of SKorean shellfish from market because of possible norovirus contamination. The Food and Drug Administration (FDA) is urging food distributors, retailers, and food service vendors to remove all shellfish imported from South Korea from the market because of possible contamination with human waste and norovirus, the Associated Press reported June 14. The decision follows an FDA evaluation that determined the Korean Shellfish Sanitation program no longer meets adequate sanitation controls. The federal agency is in ongoing discussions with South Korean authorities to resolve the issue. An FDA spokesman said June 14 the decision to call for the removal of the mollusks from the market began with norovirus outbreaks in November and December 2011. Source:

http://www.washingtonpost.com/politics/fda-urges-removal-of-skorean-shellfish-from-market-because-of-possible-norovirus-contamination/2012/06/14/gJQAjMTVdV_story.html

New foot-and-mouth disease vaccine gets licensed for use on cattle. DHS announced recently the world's first molecular foot-and-mouth (FMD) vaccine was granted conditional license for use in cattle by the U.S. Department of Agriculture (USDA) Animal and Plant Health Inspection Service's Center for Veterinary Biologics, Agri-View reported June 13. Developed at DHS's Science and Technology Directorate Plum Island Animal Disease Center (PIADC), this is the first licensed FMD vaccine that can be manufactured on the U.S. mainland. It does not require expensive, high-containment facilities because it does not use the infectious materials of the live FMD virus. DHS PIADC is working with the animal health vaccine manufacturer Merial to review the production process. Source: http://www.agriview.com/briefs/livestock/new-foot-and-mouth-disease-vaccine-gets-licensed-for-use/article_617ea396-b566-11e1-8d2f-0019bb2963f4.html

Corn crop off to a dry start, but strengthening El Nino may help. An early and unusually warm spring has morphed into a dry start for the 2012 corn and soybean crops, and the National Drought Monitor has shown progressively deteriorating conditions across much of the United States, Drovers CattleNetwork reported June 13. However, meteorologists believe conditions could improve for the U.S. Corn Belt over the next 2 weeks. They said the jet stream pattern suggest a favorable shift toward wetter conditions. Recent reports, however, show how quickly the crop is declining. The U.S. Department of Agriculture reported 66 percent of the U.S. corn crop was rated good or excellent in the week of June 4, a decline from 72 percent earning those ratings the previous week and 77 percent 2 weeks ago. Meteorologists also believe the strengthening El Nino in the Pacific Ocean could ease dry conditions in the United States. Source: http://www.agprofessional.com/news/Corn-Belt-dry-but-strengthening-El-Nino-may-help--158629985.html

FDA improves adulterated foods tracking system. The U.S. Food and Drug Administration (FDA) took steps in June to improve its ability to track patterns in food adulteration with its Reportable Foods Registry (RFR), Food Safety News reported June 13. The RFR is an online portal where companies are required to report foods they have manufactured that may be dangerous to human or animal health. Public health officials may also report food adulteration. The FDA is updating the RFR questionnaire so it can gather more detailed data about each case to gain insight into how adulteration occurs. The goal is to find trends to help the FDA figure out the most effective ways to focus its limited inspection resources to prevent problems. The new data fields in RFR allow reporters to input the specific agent of contamination, and in the case of bacterial contamination, asks whether a bacterial isolate is available. It also requests more details about the product in question and asks reporters whether the product has been removed from the market. The FDA said the data from RFR will help it respond to recall situations more efficiently. Source: http://www.foodsafetynews.com/2012/06/fda-improves-adulterated-foods-tracking-system/

Watch out for these early-season issues. A combination of a warm winter, early planting window, and a dry, hot start to summer has caused some crop diseases and issues to blow up in parts of the Corn Belt, specialists said, according to Agriculture.com June 11. The good news is the hot, dry weather has kept some more common diseases at bay more than usual, said a University of Illinois crop scientist. Things like leaf blight and spot, in corn and soybeans, have affected fewer plants in 2012 on account of the weather. However, the weather has also helped others thrive. For example, Goss's Wilt in corn, in a normal year, early June's typically too early for this disease to become a problem. However, agronomists in Nebraska said 2012 has been different. Also there are conditions that, though not technically diseases, have taken their toll on the corn crop. Rootless corn syndrome has been an issue from the Plains to the eastern Corn Belt. Caused most often by dry conditions at and following planting, the syndrome causes both stunted and altogether failed root development, and it has been showing up a lot more than normal in 2012. Source: http://www.agriculture.com/news/crops/watch-out-f-se-earlyseason-issues_2-ar24648

(California) **CA recalls more farmers market soups for botulism potential.** The California Department of Health (CDPH) warned consumers not to eat certain soups sold at southern California farmers markets because they may have been produced in a way that makes them susceptible to Clostridium botulinum. CDPH said June 11 canned soups manufactured by Malibu-based One Gun Ranch and Santa Barbara-based Organic Soup Kitchen had the potential to be contaminated with the bacteria. The soups from One Gun Ranch subject to the warning include: Campfire Kitchen Cauliflower Soup, Heirloom Tomato Fennel Gaspacho Soup, Sequoia's Skinny Spiced Coconut, Parsnip, and Tumeric Soup, Oassian's Pumpkin Stew, and Freddy's Firegrilled Meatballs. The soups were sold only at the Pacific Palisades Farmers Market in Pacific Palisades May 13 and June 3. The soups from Organic Soup Kitchen were sold at two farmers markets: the Calabasas Farmers Market and the Studio City Farmers Market in Studio City. They were sold between June 6, 2011 and May 6. The affected soups include: Fire Roasted Yam, Curried Potato Leek, Curry Lentil Bisque, Tomato Bean and Wild Herb, and Mediterranean Chipotle Chili. The health department said it is working with both companies to make sure all the products in question are removed from sale.Source: http://www.foodsafetynews.com/2012/06/ca-recalls-more-farmers-market-soups-for-botulism-potential/

Global food-trade network vulnerable to fast spread of contaminants. Two University of Notre Dame network physicists, in collaboration with food science experts, recently published an analysis of the international food-trade network that shows the network's vulnerability to the fast spread of contaminants as well as the correlation between known food poisoning outbreaks and the centrality of countries on the network, Homeland Security News Wire reported June 11. As the world's population climbs past 7 billion, the sustainable production and distribution of food is balanced against the need to ensure its chemical and microbiological safety. By 2030, food demand is expected to increase by 50 percent. Global food transport has been increasing at an exponential rate since the 1960s — faster than food production itself. As the system grows, so does pressure on regulation and surveillance organizations to track contaminants and prevent deadly outbreaks. A news release noted the paper does not predict

an increase in food poisoning cases, but it does predict significant delays with serious potential consequences in the identification of the outbreaks' sources. It calls for an interdisciplinary and incentivized approach to the understanding of the international agro-food trade network that will build on its identification of the network's critical spots. Source: http://www.homelandsecuritynewswire.com/dr20120611-global-foodtrade-network-vulnerable-to-fast-spread-of-contaminants

Government Sector (including Schools and Universities)

Pentagon crackdown on free guns riles some police. The Defense Department recently warned State law enforcement officials to track down every gun, helicopter, and Humvee the military gave them under a $2.6 billion surplus program, or have their access to the handouts cut off, the Associated Press reported June 9. A spokesman for the Defense Logistics Agency said all weapons will be withheld until the accounting is completed. According to the States, at least some of them already turned over that data. Associated Press inquiries into how the program is administered in all 50 States and several U.S. territories show most of them only keep paper records, and the few States that keep electronic records only recently made the switch from paper. "That's the problem with the entire program is it's paper-based when it should be automated," said a Michigan National Guard master sergeant, who is the State's coordinator. Source: http://www.google.com/hostednews/ap/article/ALeqM5jusRVBGdpFk0MvmPh6U03lEHfTCg?docId=a5495e8a08e3448b9878cdb80067f5c6

Information Technology and Telecommunications

'State-sponsored attackers' using IE zero-day to hijack Gmail accounts. Microsoft and Google warned about a new Internet Explorer (IE) zero-day vulnerability being exploited to hack into Gmail accounts. The browser flaw, which is currently unpatched, exposes Windows users to remote code execution attacks with little or no user action (drive-by downloads if an IE user visits a rigged site). Microsoft's advisory speaks of "active attacks" and follows a separate note from Google that references the IE flaw "being actively exploited in the wild for targeted attacks." A source close to the investigations confirms these attacks prompted Google's recent decision to warn Gmail users about "state-sponsored attackers." Internet Explorer users should know this vulnerability is different from another under-attack issue fixed June 12 with the MS12-037 bulletin. Source: http://www.zdnet.com/blog/security/state-sponsored-attackers-using-ie-zero-day-to-hijack-gmail-accounts/12462

LulzSec Reborn leaks 10,000 Twitter accounts. LulzSec Reborn leaked approximately 10,000 Twitter usernames and passwords of members who used TweetGif, an animated Gif-sharing application. The file contained much information on each member including: usernames, passwords, real names, locations, bios, avatars, secret tokens used to authenticate TweetGif to pull Twitter data, and even their last tweet. The hackers' motivations are unclear at this point;

an announcement posted on Pastebin merely linked to a destination for people to download the .SQL file. TweetGif lets users post and share animated Gif cliparts, but users have to log in through Twitter. It appears to be a relatively small application with less than 75,000 visitors globally, according to its Flag Counter stats, and only 690 followers of its Twitter account @TweetGif. Not all third-party Twitter applications use best practices to secure user data. An Imperva report indicated approximately three-quarters of Web applications may be vulnerable to remote file inclusion attacks because they include insecure tools that allow users to upload user-generated content, such as images and videos. Source: http://securitywatch.pcmag.com/none/298936-lulzsec-reborn-leaks-10-000-twitter-accounts

James Bond-style malware targets firm that secures industrial systems. A malware-based espionage campaign was recently perpetrated against Digital Bond, a security consultancy that specializes in safeguarding computer systems used to control dams, gasoline refineries, and other critical infrastructure against attack. An e-mail that addressed a Digital Bond employee by name used an account registered to appear as if it belonged to the company's founder and CEO. According to a blog post published the week of June 4, the message made reference to a paper the executive co-authored in 2009 and asked the employee to click on a Web link that led to a compressed file stored on a compromised server. Malicious code in the file installs a remote backdoor on end-user machines. It was detected by only 7 of 42 antivirus products. That suggests the trojan did not circulate widely before it targeted Digital Bond. Source: http://arstechnica.com/security/2012/06/jamesmalware-targets-industrial-systems-experts/

BIG-IP network appliances remote access vulnerability. Networking equipment specialist F5 Networks warned users about a security vulnerability in its network appliance — including its flagship BIG-IP family of products — that could allow a remote attacker to gain root access via SSH on some devices. A full list of affected firmware versions is given in the security advisory. Firmware upgrades that close the security hole are available; users who cannot upgrade to a non-vulnerable version are advised to reconfigure SSH access on their systems. Source: http://www.h-online.com/security/news/item/BIG-IP-network-appliances-remote-access-vulnerability-1615947.html

Simple authentication bypass for MySQL root revealed. Exploits for a recently revealed MySQL authentication bypass flaw are now in the wild, partly because the flaw is simple to exploit to gain root access to the database, experts said. The only mitigating factor appears to be that it depends on the C library with which the MySQL database was built. The bypass, assigned the vulnerability ID CVE-2012-2122, allows an attacker to gain root access by repeatedly trying to login with an incorrect password. Each attempt has a 1 in 256 chance of being given access. Source: http://www.h-online.com/security/news/item/Simple-authentication-bypass-for-MySQL-root-revealed-1614990.html

National Monuments and Icons

US wildfires fuel urgency for forest restoration. As firefighters battle blazes in New Mexico and Colorado that have forced evacuations and destroyed hundreds of structures, the U.S. Forest

Service chief is renewing his call to restore forests to a more natural state, where fire was a part of the landscape, the Associated Press reported June 14. Experts say a combination of decades of vigorous fire suppression and the waning of the timber industry over environmental concerns has left many forests a tangled, overgrown mess, subject to the kind of super-fires now regularly consuming hundreds of homes and millions of acres. The plan calls for accelerating restoration programs — everything from prescribed fire and mechanical thinning — by 20 percent each year in key areas that are facing the greatest danger of a catastrophic fire. The goal was set at 4 million acres with a budget of approximately $1 billion. The accelerated restoration effort is focused on several landscape-scale projects, the largest of which is a 20-year plan that calls for restoring 2.4 million acres across four forests in northern Arizona. Source: http://www.foxnews.com/us/2012/06/14/us-wildfires-fuel-urgency-for-forest-restoration/

Feds scrambing for more wildfire air resources. The week of June 11, the U.S. Forest Service (USFS) said it mobilized eight additional aircraft to ensure that an adequate number of airtankers were available for wildland firefighting efforts. With these additional airtankers, the USFS has 16 large airtankers, and one very large tanker available immediately for wildfire suppression. The USFS can mobilize an additional 11 large airtankers, should circumstances require it. Additionally, it and the Department of the Interior fire agencies can mobilize hundreds of helicopters and dozens of smaller aircraft, called "single-engine airtankers." The U.S. President authorized the USFS to expedite its acquisition of at least seven next-generation large air tankers via Senate Bill 3261, which passed the U.S. Senate and the U.S. House of Representatives the week of June 4. As of June 13, 19 active large fires were burning in 9 States, including one of the largest wildfires in New Mexico history, and one of the largest wildfires on record in Colorado. While extremely serious fires were burning in several States, the season was considered below average, meaning that additional resources remained available if needed. Source: http://summitcountyvoice.com/2012/06/14/feds-scrambing-for-more-wildfire-air-resources/

Rapidly spreading wildfires choke Colo., N.M. Authorities in Colorado and New Mexico battled wildfires spreading rapidly through mountainous forest land that forced hundreds of evacuations and destroyed dozens of structures, the Associated Press and CBS News reported June 11. A wildfire burning in a mountainous area 15 miles west of Fort Collins, Colorado, nearly doubled to 58 square miles, forcing hundreds of evacuations, and destroying at least 18 structures. June 11, the Larimer County Sheriff's Office said 400 people were fighting the fire. The U.S. Forest Service said a federal team was slated to take over management of the fire. Strong winds grounded an aircraft fighting a 40-square-mile wildfire near Ruidoso, New Mexico. Crews were working to build a fire line around the fire, which started June 8 and damaged or destroyed 36 structures. A spokesman for the New Mexico State Forestry Division said the number of Ruidoso evacuees was in the hundreds. Both fires were dwarfed by the Whitewater-Baldy fire in southwest New Mexico — the largest in the State's history — that charred 450 square miles of wilderness forest since mid-May. Firefighters June 10 battled a wildfire that blackened 6 square miles in Wyoming's Guernsey State Park and forced the evacuation of between 500 and 1,000 campers and visitors. Authorities told people in Hartville to be ready to

evacuate. In Colorado, the High Park Fire burned more than 20,000 acres, and up to 2,600 people were evacuated. Cooler weather helped firefighters in their battle against two wildfires in Utah. Firefighters said the Box Creek wildfire, which grew to 2,000 acres June 11, was 75 percent contained and would likely be fully controlled by June 12. Source: http://www.cbsnews.com/8301-201_162-57450164/rapidly-spreading-wildfires-choke-colo-n.m/

Postal and Shipping

(California) **Would-be mail thief prompts bomb scare.** A would-be mail thief prompted a bomb scare June 8 outside the Perris Union High School District offices in Perris, California, authorities said. Someone reported a small, suspicious package on a blue U.S. Postal Service mailbox outside the offices, according to a Riverside County Sheriff's Department news release. It was wrapped in electrical and duct tape and had two cords attached to it that were running into the mailbox slot. Deputies called in the sheriff's hazardous device team. The area was cordoned off and workers in offices near the mailbox were evacuated to another part of the property. The package turned out to be harmless. The other ends of the cords were attached to a VHS tape covered in a sticky substance apparently intended to fish letters out of the mailbox. The would-be thief evidently had abandoned the effort, leaving his fishing device. Source: http://www.pe.com/local-news/riverside-county/perris/perris-headlines-index/20120608-perris-would-be-mail-thief-prompts-bomb-scare.ece

Public Health

Software update site for hospital respirators found riddled with malware. A Web site used to distribute software updates for a wide range of medical equipment has been blocked by Google after it was found to be riddled with malware and serving up attacks, Threatpost reported June 14. The site belongs to San Diego-based CareFusion Inc., a hospital equipment supplier. The infected Web sites, which use many different domains, distribute firmware updates for a range of ventilators and respiratory products. Scans by Google's Safe Browsing program in May and June found the sites were rife with malware. About 6 percent of the 347 Web pages hosted at Viasyshealthcare(dot)com, a CareFusion Web site used to distribute software updates for the company's AVEA brand ventilators, were found to be infected and pushing malicious software to visitors' systems. The software downloaded from Viasyshealthcare(dot)com included 48 Trojan horse programs and 2 scripting exploits, according to a review of the Google Safe Browsing report by Threatpost. Another domain, sensormedics(dot)com, which supports CareFusion's VELA brand ventilators, was also found to be serving "content that resulted in malicious software being downloaded and installed without user consent," according to a June 13 scan by Google's Safe Browsing crawler. CareFusion removed links to the infected Web sites hosting software updates for the respirators from its Product Support page. However, the company still offered links for parts and supplies for CareFusion's 3100A High Frequency Oscillatory Ventilator and LTV series ventilators that were likewise infected, according to Google. Source: http://threatpost.com/en_us/blogs/software-update-site-hospital-respirators-found-riddled-malware-061412

F.D.A. investigates fresenius for failure to warn of risk. The New York Times reported June 14 the Food and Drug Administration (FDA) is investigating whether the nation's largest operator of dialysis centers violated federal regulations by failing to inform customers of a potentially lethal risk connected to one of its products. The German-based company, Fresenius Medical Care, treats more than a third of the estimated 400,000 Americans receiving dialysis. It also is the leading supplier of dialysis machines and disposable products, which are used by many clinics in addition to its own. In November 2011, Fresenius's medical office sent an internal memo to doctors in the company's dialysis centers, warning them that failure to properly use one of the company's products appeared to be contributing to a sharp increase in the risk of patients dying suddenly from cardiac arrest. However, Fresenius did not immediately warn other centers that use the product, which is known as GranuFlo. It did so only in late March after the FDA received, anonymously, a copy of the internal memo and asked the company about it. The chief medical officer for Fresenius in North America said his office, which wrote the memo, was in charge of the company's own centers and had no way of communicating with noncompany clinics except through papers in medical journals. He said the findings of the internal memo were too preliminary to warrant a publication. After Fresenius notified its customers in late March, the FDA issued an alert in late May that applied to all products such as GranuFlo. Source: http://www.nytimes.com/2012/06/15/health/fda-investigates-fresenius-for-failure-to-warn-of-risk.html

APhA: No credit card data obtained by hackers. The official Web site of the American Pharmacist Association (APhA) was restored after Anonymous-affiliated hackers breached the site forcing the organization to take it offline, Softpedia reported June 11. According to a statement posted on the re-launched site, there is no indication that the attackers accessed sensitive information such as credit card data. The organization said the hackers leaked e-mail addresses, names, and physical addresses, details that could be used by cybercriminals to initiate phishing campaigns with the purpose of gathering sensitive data. At the time of the incident, the hackers leaked around 64 megabytes of information from the site's databases, but they also claimed to have obtained 16,000 patient records. While APhA and law enforcement continue to investigate the incident, security measures were enhanced to prevent the Web site from falling victim to future attacks. Source: http://news.softpedia.com/news/APhA-No-Credit-Card-Data-Obtained-by-Hackers-274820.shtml

Transportation

Nothing Significant to Report

Water and Dams

(Wisconsin) **DNR: 2 sand mining companies are polluters.** The Wisconsin Department of Natural Resources (DNR) asked the State Department of Justice (DOJ) to prosecute two silica sand mining companies for pollution violations in Minnesota and Wisconsin, the Associated Press reported June 11. The DNR alleges Preferred Sands of Minnesota failed to have a storm

water pollution prevention plan in place when a dike embankment collapsed at a Trempealeau County mine. The March 3 collapse sent more than 2,100 feet of river mud into privately-owned land. The Eau Claire Leader-Telegram said the DNR is also recommending Interstate Energy Partners and Tiller Corp. be prosecuted for failing to maintain dikes and berms around a Burnett County, Wisconsin mine where muddy water flowed into a creek entering the St. Croix River. Source: http://www.wxow.com/story/18757503/dnr-2-sand-mining-companies-are-polluters

Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168